NEWS
Cyber Security
Vol. 3 | Issue 4 April 2018

IC3 | Dark Web | 911 | AVCrypt | Atlanta | Facebook | Russia | Stats | Challenge

Hello everyone and welcome to this month's TXDPS Cyber Newsletter.

It is that time of year again. Everyone's favorite time where we get to fill out our taxes. :) It is also a favorite time of year for phishing scams pretending to be from the IRS. Remember that the IRS will not initiate contact via email about a bill or tax return. Below are some of this year's "Dirty Dozen" scams according to the IRS.

Phishing: Taxpayers should be alert to potential fake emails or websites looking to steal personal information. The IRS will never initiate contact with taxpayers via email about a bill or tax refund. Don't click on one claiming to be from the IRS. Be wary of emails and websites that may be nothing more than scams to steal personal information. (IR-2018-39)

Phone Scams: Phone calls from criminals impersonating IRS agents remain an ongoing threat to taxpayers. The IRS has seen a surge of these phone scams in recent years as con artists threaten taxpayers with police arrest, deportation and license revocation, among other things. (IR-2018-40)

Identity Theft: Taxpayers should be alert to tactics aimed at stealing their identities, not just during the tax filing season, but all year long. The IRS, working in the Security Summit partnership with the states and the tax industry, has made major improvements in detecting tax return related identity theft during the last two years. But the agency reminds taxpayers that they can help in preventing this crime. The IRS continues to aggressively pursue criminals that file fraudulent tax returns using someone else's Social Security number. (IR-2018-42)

Return Preparer Fraud: Be on the lookout for unscrupulous return preparers. The vast majority of tax professionals provide honest, high-quality service. There are some dishonest preparers who operate each filing season to scam clients, perpetuating refund fraud, identity theft and other scams that hurt taxpayers. (IR-2018-45)

Fake Charities: Groups masquerading as charitable organizations solicit donations from unsuspecting contributors. Be wary of charities with names similar to familiar or nationally-known organizations. Contributors should take a few extra minutes to ensure their hard-earned money goes to legitimate charities. IRS.gov has the tools taxpayers need to check out the status of charitable organizations. (IR-2018-47)

Inflated Refund Claims: Taxpayers should take note of anyone promising inflated tax refunds. Those preparers who ask clients to sign a blank return, promise a big refund before looking at taxpayer records or charge fees based on a percentage of the refund are probably up to no good. To find victims, fraudsters may use flyers, phony storefronts or word of mouth via community groups where trust is high. (IR-2018-48)

To see the rest of the "Dirty Dozen", click **HERE**.

You can find other good information to help keep you safe from IRS scans this year by clicking **HERE**.

I suggest you also watch this **video** on YouTube as well as this **video**.

Cyber News!!

Impersonation of the Internet Crime Complaint Center

Cyber actors are scamming victims into providing personal information and downloading malicious files by impersonating the Internet Crime Complaint Center (IC3). In a recent scam, the unknown actors emailed victims requesting the recipients provide additional information in order to be paid restitution. In an attempt to make the emails appear legitimate, the scammers included hyperlinks of news articles which detailed the arrest or apprehension of an internet fraudster. The unknown actors also attached a text document (.txt) to download, complete, and return to the perpetrators. The text file contained malware which was designed to further victimize the recipient.

Click **HERE** to read more.

Your online identity sells for exactly $1,170 on the dark web — here's how to block the sale

(Fox News) - What is the asking price for your online identity? Now, we finally know.

Harvesting a few of your credit cards, your social security number, your billing address, and even the names of your children now has an exact price tag, almost like an Amazon shopping list. According to a new study by Privacy Central, it's exactly $1,170 on the dark web.

Like an auction site or Craigslist, the Dark Web is a shopper's paradise for hackers.

Netflix accounts, an Uber login, and access to your AirBnB credentials come cheap -- $10 each. And, how about your Gmail login? That sells for about a dollar. How about your iTunes account info? That's exactly $15.38. PayPal account? $247.

Click **HERE** to read more.

Baltimore 911 dispatch system hacked, investigation underway, officials confirm

(Orlando Sentinel) - Baltimore's 911 dispatch system was hacked by an unknown actor or actors over the weekend, prompting a temporary shutdown of automated dispatching and an investigation into the breach, Mayor Catherine Pugh's office confirmed Tuesday.
James Bentley, a spokesman for Pugh, confirmed that the Sunday morning hack affected messaging functions within the computer-aided dispatch, or CAD, system, but said the mayor would not otherwise comment on the matter Tuesday.

Dave Fitz, an FBI spokesman, said his agency was aware of the breach and provided some technical assistance to the city.

City personnel "identified a limited breach" of the CAD system, which supports the city's 911 and 311 services, about 8:30 a.m. Sunday, Frank Johnson, chief information officer in the Mayor's Office of Information Technology, said in a statement.

Click **HERE** to read more.

More Cyber News!!

AVCrypt ransomware attempts to eradicate your antivirus

(ZDNet) - A new type of ransomware which tries to uninstall security software on victim PCs has been discovered in the wild.

The ransomware, dubbed AVCrypt, was first discovered by MalwareHunterTeam and later analyzed by security professionals at Bleeping Computer.

According to an analysis of the malware, AVCrypt will attempt to not only remove existing antivirus products before encrypting a compromised computer but will also delete a selection of Windows services.

Researchers Lawrence Abrams and Michael Gillespie say that the ransomware "attempts to uninstall software in a way that we have not seen before," which marks the malware as unusual.

The true purpose of the malware -- which appears to be ransomware due to its capabilities -- is also in question, as some elements appear unfinished. There are elements of encryption, but no true ransom note, and together with AVCrypt's process deleting, it is possible the malware may also be utilized as a wiper.

Click **HERE** to read more.

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

(CNN) - Residents can't pay their water bill or their parking tickets. Police and other employees are having to write out their reports by hand. And court proceedings for people who are not in police custody are canceled until computer systems are functioning properly again.

More than six days after a ransomware attack shut down the city of Atlanta's online systems, officials here are still struggling to keep the government running without many of their digital processes and services.

The city said on Twitter that all court dates set for Wednesday will be rescheduled and all applications for jobs with the city are suspended until further notice.

On Tuesday officials told city employees to turn their computers and printers back on for the first time, part of an ongoing assessment of the impact of the cyber breach, which took place on March 22.

The city also said on Twitter Wednesday that "there is no evidence to show that customer or employee data has been compromised." But city officials have urged employees and customers to contact credit agencies and monitor their bank accounts as a precaution.

Click **HERE** to read more.

More Cyber News!!

It's not just Facebook. Thousands of companies are spying on you.

(CNN) - In the wake of the Cambridge Analytica scandal, news articles and commentators have focused on what Facebook knows about us. A log, it turns out. It collects data from our posts, our likes, our photos, things we type and delete without posting, and things we do while not on Facebook and even when we're offline. It buys data about us from others. And it can infer even more: our sexual orientation, political beliefs, relationship status, drug use, and other personality traits — even if we didn't take the personality test that Cambridge Analytica developed.

But for every article about Facebook's creepy stalker behavior, thousands of other companies are breathing a collective sigh of relief that it's Facebook and not them in the spotlight. Because while Facebook is one of the biggest players in this space, there are thousands of other companies that spy on and manipulate us for profit.

Harvard Business School professor Shoshana Zuboff calls it "surveillance capitalism." And as creepy as Facebook is turning out to be, the entire industry is far creepier. It has existed in secret far too long, and it's up to lawmakers to force these companies into the public spotlight, where we can all decide if this is how we want society to operate and — if not — what to do about it.

Click **HERE** to read more.

Here Are The Clever Means Russia Used To Hack The Energy Industry

(Forbes) - Last July, officials from the Federal Bureau of Investigation and the Department of Homeland Security revealed that Russian hackers were behind cyber intrusions into the U.S. energy power grid. The intrusion illustrated the severe threat that hackers pose to our most critical industries—energy, finance, healthcare, manufacturing and transportation.

The DHS and FBI downplayed the danger in a joint statement: "There is no indication of a threat to public safety, as any potential impact appears to e limited to administrative and business networks.

But that might not be the end of it. Russia may be laying the groundwork for more damaging hacks, on America as well as other nations, using new cyber weapons like CrashOverride and BlackEnergy 3.

In 2015, Russia tested this on the Ukrainian capital of Kiev. These tools were specifically developed to disrupt electric power grids and it blacked out 225,000 people in the Ukraine.

One might wonder what is Russia's end game for this kind of attack.
To hurt us financially? To show us how vulnerable we are? In preparation for a more sinister attack?

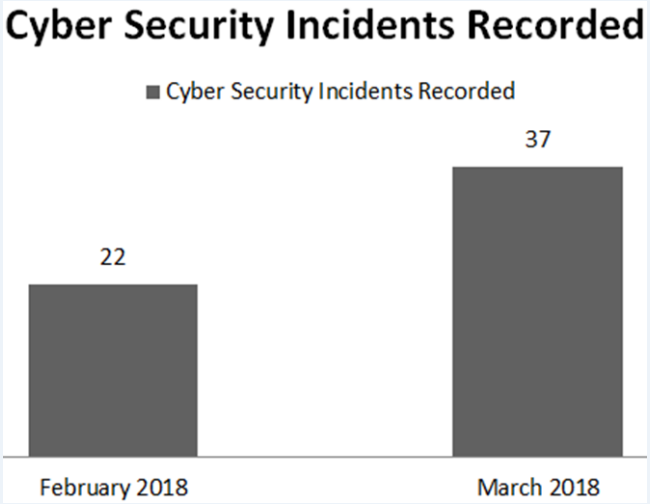
Is it to punish American for anti-Russian policies? The White House expelled 60 Russians from the United States this week, joining western allies in response to Russia's poisoning of a former Russian spy in Britain with what was a banned chemical weapon.

Click **HERE** to read more.

<Cyber Stats for Jan and Feb>

Email Security	February 2018	% Change	March 2018
Phishing attacks against agency	7	142.86%	17
Emails inspected by sensors	1,629,735	-100.00%	Pending Code
Emails blocked by sensors	1,602,827	-100.00%	Pending Code
DPS Custom Email Threat Signatures Created	12	-83.33%	2

In this month's stats, you see Phishing attacks more than doubled in March while malware threats stayed relatively equal to the previous month. Phishing attempts can often lead to malware infecting your computer. Test your knowledge on phishing emails in the Cyber Challenge to see how good you are at determining a legitimate email from a phishing attempt.



As you can see from the above graph, our cyber incidents significantly increased. While this has the appearance of being bad, it really isn't. The graph just proves how great a job our IT and Cyber Operations teams are doing to protect the agency. It also shows vigilance from users. Your continued cyber vigilance not only protects the agency but also helps keep you safe. Keep up the good work.

Please let me know if there are topics or metrics you would like to see me try to include in future newsletters. Also, if you have a cyber related story you would like to share, please do so. With your permission I might just include it in future newsletters.

Cyber Challenge

Cyber Challenge

Were you able to figure out the messages in last month's newsletter?

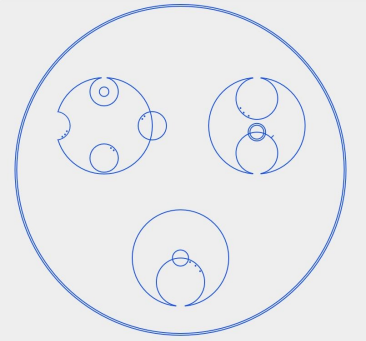
In last month's newsletter I provided two challenges. The first was where Cyber Challenge is on this newsletter. The characters were in Wingdings 3. Once you converted the characters to English you were provided with a group of Hexadecimal numbers which when converted give you the message:

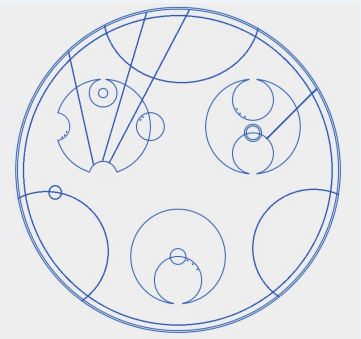
Cyber Challenge

"Braces are not suspenders"

I would like to congratulate **Rene Hess** for being the first person to figure out that message.

The second message was a picture that I provided. It was a phrase translated into a fictitious circular language known as Gallifreyan, and is the language of the Time Lords from Dr. Who. The message said Do Good Cyber and **Erich Neumann** was the first to figure out the message. In fact, he even corrected me and provided the correct message. The picture on the left is the message I provided and the one on the right is from Erich.





To follow inline with the theme of protecting yourself from phishing scams, this month's Cyber Challenge is not really a challenge but more an online training exercise. To do it, go to PhishingBox at this link:

https://www.phishingbox.com/phishing-iq-test

To evaluate how well you can identify a phishing attempt from a legitimate email. You don't have to, but feel free to email me and let me know how you did.

Kirk